InstantWave™ *High Rate*

11Mbps Wireless Networking

Access Point

User's Guide

Rev. A1
December 2001

NWH650

National Datacomm Corporation
4F, No. 24-2, Industry East 4th Road, Science Park
Hsin-Chu, Taiwan, R.O.C.

Technical Support
E-mail: techsupt@ndc.com.tw

NDC World Wide Web
www.ndc.com.tw

TRADEMARKS

NDC and InstantWave are trademarks of National Datacomm Corporation. All other names mentioned in this document are trademarks/registered trademarks of their respective owners.

NDC provides this document "as is", without warranty of any kind, neither expressed nor implied, including, but not limited to, the particular purpose. NDC may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time. This document could include technical inaccuracies or typographical errors.

FCC WARNING

This equipment has been tested and found to comply with the limits for a Class B Digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Packing List

The package should contain the following items:

- One NWH650 InstantWave High Rate Access Point
- One RS-232 Cable
- One RJ-45 Cable
- One Power Adapter
- One CD ROM (Contains drivers, Station utilities, Access Point management tools, Network Profile Manager, User’s Guides, links to online resources

Table of Contents

List of Figures

Introduction

Congratulations on choosing one of NDC's InstantWave High Rate wireless networking products. InstantWave High Rate was one of the first IEEE 802.11b wireless standard compliant products in the industry and was designed to maximize the convenience of networking. You will find InstantWave High Rate products very easy to setup and use.

The User's Guide gives comprehensive instructions on installing and using the InstantWave NWH650 High Rate Access Point (AP). The AP provides a transparent bridged connection between a wired network and a wireless network and allows your wireless stations to communicate with devices attached to your wired network. It manages the flow of data packets from the wired LAN to the wireless LAN, and vice versa. The Access Point Management System (APMS) performs wireless network configuration management and diagnostic functions.

InstantWave High Rate Family

The InstantWave NWH650 High Rate Access Point is part of a family of easy to use high performance wireless communication products. The family products include:

- InstantWave High Rate Access Points (NWH650, NWH660)
- InstantWave High Rate PCI Card (NWH630)
- InstantWave High Rate PC Card (NWH610)

System Requirements

System requirements to install and operate the InstantWave High Rate Access Point are:

- One PC
- One 802.11b compliant card
- An Ethernet drop (UTP)
- An RS-232 cable (only used when configuration of the AP's network properties is necessary)
- A PC (only used when configuration of the AP's network properties is necessary)

Cabling

Connecting the Access Point (AP) to an Ethernet network requires an Unshielded Twisted-Pair cable. The AP fits into the network just as any other node would do. An LED will light to indicate a connection. The cable length should follow Ethernet standards in each case.

How to Use this Guide

InstantWave High Rate is extremely versatile in providing varying levels of network management. For Small Office/Home Office users, setup and configuration is a quick, four-step process. The Access Point Hardware Installation section, on page 8, provides simple instructions to get your network up and running within minutes. Go to the Access Point Hardware Installation section if your network will meet the following criteria:

- You will accept all default values
- Your network will have only one Access Point

The AP COMFig tool, see page 11, permits AP configuration from a PC via a COM port connection. The program enables the user to change the default Access Point IP configuration settings before introducing a new AP to an already established wireless network.

Before using the setup tool, you should read through the next section ‘Planning Your Network’, in order to get the best possible performance from your InstantWave High Rate wireless network.

Planning Your Network

Infrastructure Network Types

An Infrastructure network is formed by several stations and one or more Access Points (APs), with the stations within a set distance from the AP. **Figure 1** depicts a typical Infrastructure network topology.

There are three infrastructure network setups that are commonly used. It is a good idea to understand the possible network setups and configuration requirements before planning your wireless network.

Type 1. The simplest wireless infrastructure network is composed of one Access Point (AP) and a few wireless Stations communicating via radio waves (**Figure 1**). This setup enables mobile stations to communicate with each other. The main benefit of this type of network is to extend the range of the network. If an AP is placed between the stations, the radio transmission distance is effectively doubled since Wireless Computer-1 can talk to Wireless Computer-2 through the AP. The drawback of this configuration is that the effective bandwidth is halved since all communication is relayed by the AP.

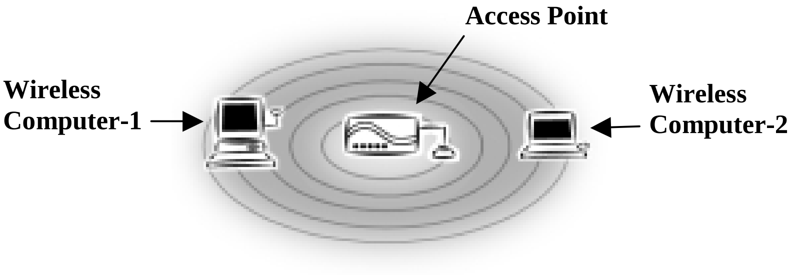


Figure 1. Simple Wireless Infrastructure Network

Type 2. The next simplest wireless network is very similar to the Type 1 network. This time the AP is connected to a wired Ethernet network as a node. In this configuration the AP is effectively performing as a bridge between the wired Ethernet and the wireless networks (**Figure 2**).

Wireless users have the same access to the network resources as they would have if they were wired. This type of network is usually used to extend an existing network into a difficult to wire or a roaming environment.

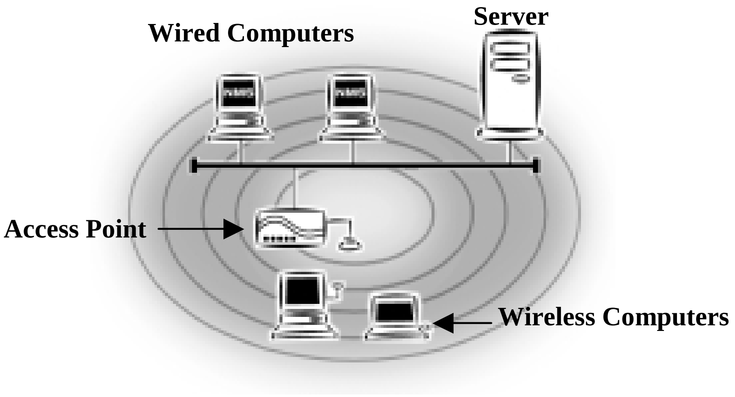


Figure 2. Single AP Network

Type 3. The third type of network is composed of multiple APs and multiple Stations (**Figure 3**).

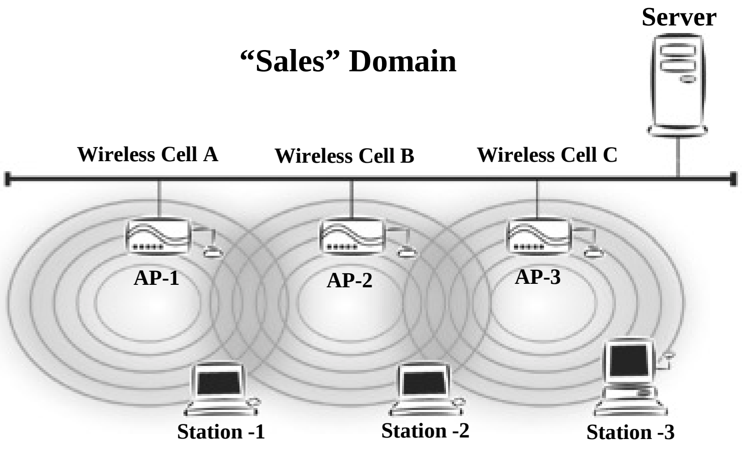


Figure 3. Multiple AP Network

The reasons for having multiple APs installed are:

1. To increase bandwidth in order to boost overall network performance
2. To extend the coverage range

Any other type of configuration is usually a mix of these commonly used types.

Planning an Infrastructure Network

This section explains some of the things you need to consider in planning an Infrastructure network. Setting up is a two step process.

1. Install and configure the InstantWave High Rate products
2. Decide the best physical location of the InstantWave High Rate products so as to optimize performance

The following sections give quick guidelines for these two steps. Before we go into detail, the network planner should first decide whether to have a single AP wireless network or a multiple APs network.

Single AP Installation

If you are setting up a simple network with only one AP and a few Stations (a Type 1 or Type 2 network configuration as described in Infrastructure Network, page 3), the installation can be performed painlessly. All you need to do is make sure the AP and all the wireless Stations hold the same 'Domain Name' in their configuration.

Adding a new Station to an existing Infrastructure network is easy. Again, all you need to do is to set the newly added Station's 'Domain Name' to the same as that of the AP's.

Multiple AP Installation

***Install multiple APs in the same network (or Domain) with an overlapping signal* (Figure 3)**

- Use the same Domain Name
- Enable the roaming function in the Station if roaming is required

Note: A Station will automatically connect to whichever AP in the same domain is offering the best signal

Roaming

InstantWave High Rate products are equipped with seamless roaming capabilities. Roaming is necessary to prevent mobile Stations from being disconnected from the network as they move around.

InstantWave High Rate is designed to allow wireless Stations to roam freely within an infrastructure domain composed of multiple APs with overlapping signal coverage (as in the Type-3 network configuration described in the previous section). For example, roaming enables Station-1 to move from the AP-1 signal coverage area to the AP-2 signal coverage area without disconnecting from the network. The handover is achieved transparently; the Station-1 user would not realize he had moved from AP-1 to AP-2.

The requirements for a roaming environment are:

a) Multiple APs with overlapping signal coverage (see Multiple AP Installation, page 5)
b) The APs must be configured to have the same Domain name (see AP COMFig/Service, page 12)
c) The mobile Stations must have the same Domain name as that of the APs
d) *It is advisable that APs on different TCP/IP subnets be given different Domain names to avoid roaming confusion (see AP COMFig/Service, page 12)

*Note: *If you want to move your mobile PC between different APs without terminating the existing networking link, you need to enable the roaming function on the Mobile Station. The APs that a Mobile Station will roam to must also be configured with the same domain name. If a Station detects that the signal quality with the current linked AP is weak, it will search for an AP in the same domain with a better signal quality and automatically establish a new connection with it. When a Station is roaming, it will always use the same IP address. The TCP/IP router will not route information packets to a Mobile Station if it re-associates with a AP that is in a different TCP/IP subnet. In other words, if your network consists of two subnets connected by a router, a Mobile Station may roam to a different subnet with the same domain name and then fail to communicate with other network devices via TCP/IP. To avoid running into such an awkward situation, you must assign different domain names to different TCP/IP subnets.*

Access Point Placement Guidelines

A characteristic of radio communication is the interference problem. Radio is receptive to interference. Therefore, the more interference you can avoid, the better performance you will get from wireless products. The following section describes how the InstantWave High Rate AP should be placed to reduce possible interference.

A few tips to mention that are particularly significant in a radio wave communications system:

1. Radio waves reflect or refract from buildings, walls, metal furniture, or other objects. This could result in performance degradation due to the fluctuation of the received signal.

2. Microwave ovens use the 2.45 GHz frequency band. InstantWave High Rate also functions in the 2.4 ~ 2.5 GHz band, and therefore shares some of the band with microwave ovens. This means that when a nearby microwave oven is in use, it may interfere with InstantWave High Rate, resulting in performance degradation on the wireless network.

Placing For Performance

For the best performance, it is advisable that users follow the guidelines below in placing the product:

- Place the AP as high as possible, in as open an area as possible
- Avoid placing the AP close to metal objects (e.g., file cabinets, metal cubicles, etc.)
- Keep APs and Stations as far away as possible from microwave ovens (10 meters min. is advisable)

Placement Tools

InstantWave High Rate includes a Station utility program to help users find the best location in which to place the AP relative to the location of the Stations.

step1. Allow a wireless Station to connect with the AP

step2. From the Station, run the InstantWave High Rate Station Monitor RF Signal Quality Program

step3. Move the AP and the AP’s antenna to find the best signal quality

Getting Started

Access Point Hardware Installation

Access Point Hardware Setup explains how to quickly setup the Access Point for use via a wired Ethernet connection, and using the factory default settings. For installation in networks using other than the default settings, i.e. into existing networks, complete the Hardware Setup and refer to Using the AP COMFig Tool, page 11. To setup a wireless station, refer to the PCI/PC Card User's Guide.

Figure 4. Access Point

step1. Connect the Ethernet network cable to the UTP port on the back panel of the Access Point.

step2. Connect the power adapter to the electricity outlet and then to the Access Point DC-In port on the back panel of the access point.

The Access Point is now ready to communicate with the wireless stations using its factory default settings. Refer to the InstantWave High Rate PCI/PC Card User's Guide for card setup instructions.

LED Indicators

The Access Point LEDs show the status of the connections. Figure 5 shows the LEDs and Figure 6 their functions.

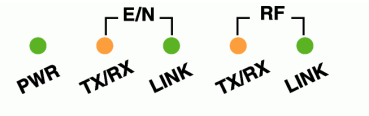


Figure 5. Access Point LEDs

General	***Color***	***Function***
PWR (Power/Status)	Green	Unlit: Power OFF Blinking: Diagnostic test On: Healthy condition
	Red	On: Abnormal Condition

E/N (Ethernet)	***Color***	***Function***
TX/RX	Orange	Blinks to indicate Ethernet transmission/reception activity
LINK	Green	Indicates an Ethernet link. If the radio fails, this LED will not light

RF	***Color***	***Function***
TX/RX	Orange	Blinks to indicate radio transmission/ reception activity
LINK	Green	Indicates a wireless link. If the radio fails, this LED will not light

Figure 6.   LED Functions

Hardware Pre-Configuration

Before adding an AP into an existing Ethernet network, you may need to set basic configurations, e.g. domain name (SSID), security setting (WEP), AP name, channel number, or IP address in order to make it compatible with the existing network.

Follow the steps below to connect the AP to a PC for configuration:

step1. Connect the supplied RS-232 cable to the COM port on the AP and connect the other end to a serial port (COM port) on the PC

step2. Power on the AP

Installing the AP Management Tools

step1. Insert the InstantWave High Rate CD into the CD-ROM drive and click ***Start/Run***. Type *e:/menu.exe* (assuming the CD drive is E) and click ***OK*** to open the InstantWave CD main menu

step2. Click ***Install AP Management Tools*** to install the *AP COMFig Tool*, *AP Management System (APMS)* and *Trap Server* utility to your system

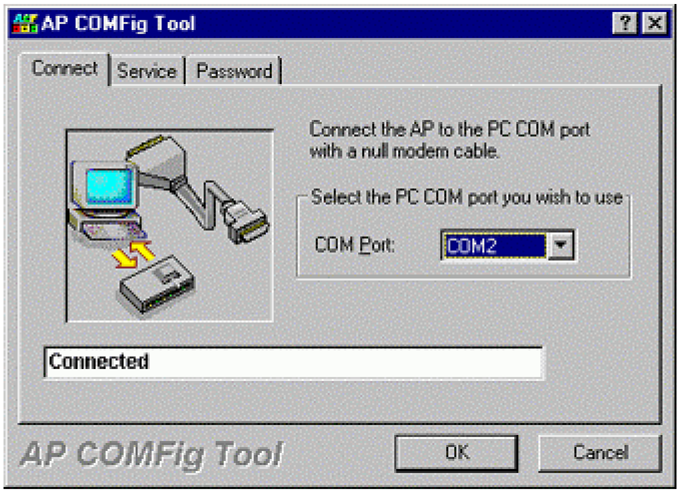
Using the AP COMFig Tool

The AP COMFig Tool is a Windows based utility used to configure the AP via a COM port connection between the AP and a PC.

It provides the following functions:

- Sets AP parameters (e.g., IP address, Domain name (SSID), Security, etc.)
- Diagnoses the AP hardware and shows the diagnostic results
- Upgrades the AP firmware
- Resets the AP Configuration
- Manages the APMS Host table

To start the AP COMFIG Tool, click ***Start/Programs/InstantWave High Rate AP/AP COMFig Tool***. The program opens with the *AP COMFig Tool/Connect* card. It will show *Connected* when a connection is made.



Connect the AP to the PC COM port with a null modem cable.

Select the PC COM port you wish to use

COM Port: COM2

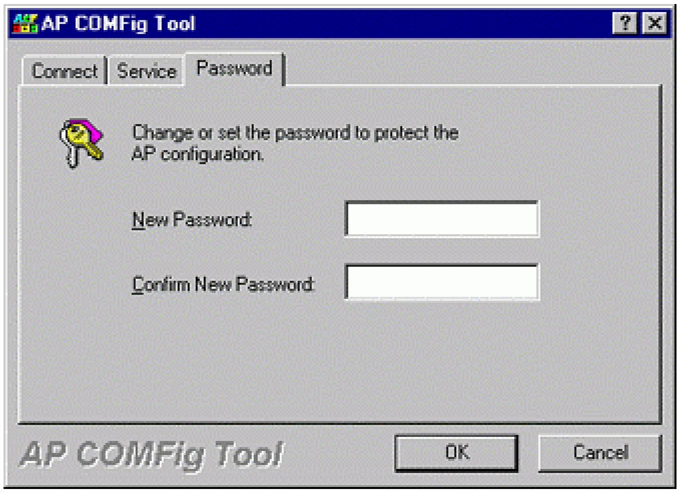
Connected

Figure 7. AP COMFig Tool/Connect

AP COMFig/Password

Click on the *Password* tab to open the *Password* card. Setting a password prevents unauthorized changes to the AP configuration settings.

Note: The password will be shared with the APMS program on the same PC.



Change or set the password to protect the AP configuration.

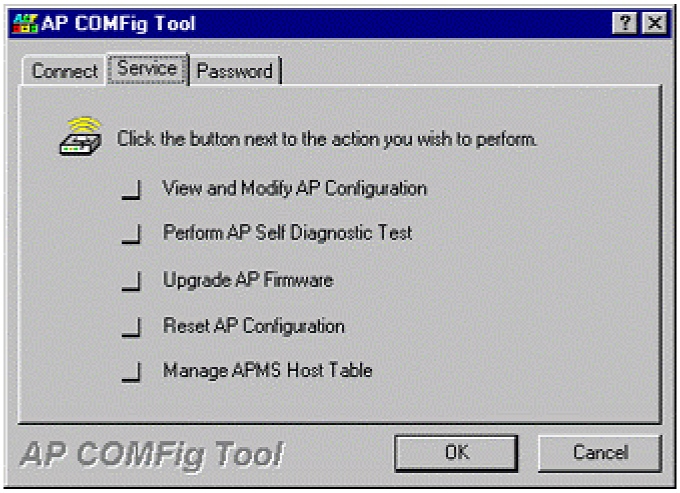
New Password:

Confirm New Password:

Figure 8. AP COMFig Tool/Password

AP COMFig/Service

After connecting with the AP, click on the *Service* tab to open the *Service* card (**Figure 9**). The *Service* card provides access to the management features.



Click the button next to the action you wish to perform.

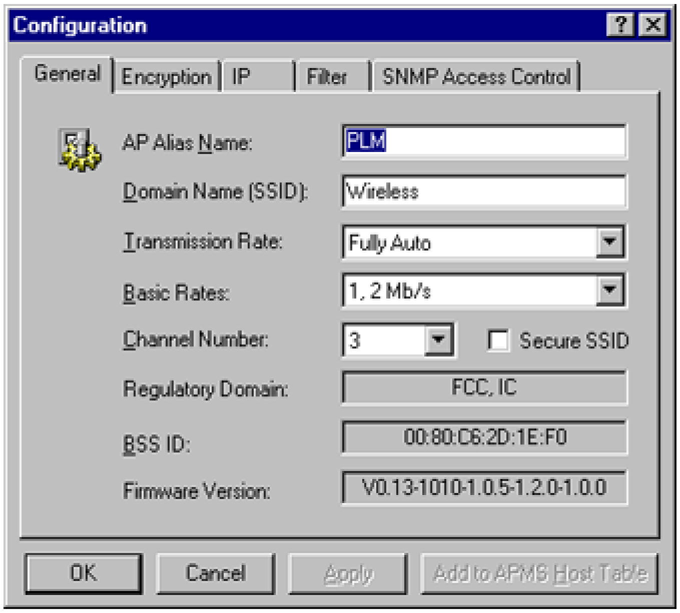
- □ View and Modify AP Configuration
- □ Perform AP Self Diagnostic Test
- □ Upgrade AP Firmware
- □ Reset AP Configuration
- □ Manage APMS Host Table

Figure 9. AP COMFig Tool/Service

Click the *View and Modify AP Configuration* button. The *Configuration* screen will open (**Figure 10**).

General:

The *General* card (**Figure 10**) is the first card in the *Configuration* section.



Configuration

AP Alias Name: PLM

Domain Name (SSID): Wireless

Transmission Rate: Fully Auto

Basic Rates: 1, 2 Mb/s

Channel Number: 3 □ Secure SSID

Regulatory Domain: FCC, IC

BSS ID: 00:80:C6:2D:1E:F0

Firmware Version: V0.13-1010-1.0.5-1.2.0-1.0.0

Figure 10. Configuration/General

On this card, you can set and view general AP settings:

AP Alias Name	Assigns the AP a unique human friendly name that allows the AP to be easily identified
Domain Name (SSID)	This is commonly called the Domain Name but is defined in the IEEE 802.11b Wireless Standard as SSID. Stations and APs in the same group must use the same Domain Name
Transmission Rate	Sets the transmission rate at which the data packets are transmitted by the AP
Basic Rates	This value determines the basic rates used and reported for this BSS by the AP. The highest rate specified will be the rate that the AP will use when transmitting broadcast/multicast and management frames. Available options are: • 1 and 2Mbps • All (1, 2, 5.5, and 11Mbps)
Channel Number	You can change the channel number from here. Refer to the Appendix, page 52, for channels supported in each regulatory domain
Secure SSID	Click to enable or disable the secure SSID option. • Blocks a connection request from a station without the correct SSID • Hides the SSID in outgoing beacon frames. A site-survey tool will not find the SSID

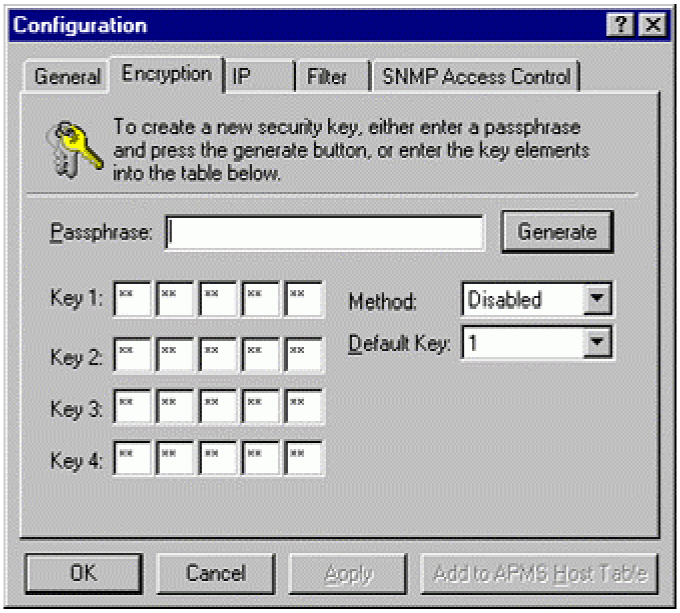
Regulatory Domain	Identifies the country where the AP is used. Each country has defined its available channel numbers and transmission power (see Appendix, page 52)
BSSID	This is the MAC ID of the AP
Firmware Version	The current AP firmware version

Important:
In a multiple cell network topology, overlapping and/or adjacent cells using different channels can operate simultaneously without interference if the frequency distance between the center frequencies is at least 30MHz. For example channels **1, 7, and 13** are non-overlapping frequency channels.

After making any changes, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

Encryption:

Data encryption provides more secure wireless data communications. Click the *Encryption* tab to setup/change the security settings (**Figure 11**). The default is *Disabled* and initially the keys section will be blank.



To create a new security key, either enter a passphrase and press the generate button, or enter the key elements into the table below.

Passphrase:

Key 1: ** ** ** ** **

Key 2: ** ** ** ** **

Key 3: ** ** ** ** **

Key 4: ** ** ** ** **

Method: Disabled

Default Key: 1

Figure 11. Configuration/Encryption

The dropdown *Method* box lists three options:

1. Disabled (default) - Disable data encryption
2. 40-bit WEP - Enable use of 40-bit WEP
3. 128-bit WEP - Enable use of 128-bit WEP

Key Generation - There are two ways to generate a security key.

The first is by entering any text in the *Passphrase* field. Click the ***Generate*** button. For 40-bit WEP, it will generate four keys, Key 1, Key 2, Key 3, and Key 4. Select a key number from the dropdown list of the *Default Key* box. If you do not manually select a key, key 1 will be selected. For 128-bit WEP, only one key will be generated. Click ***Apply***.

Another WEP key generation method is to insert the key values directly from the keyboard. Enter your own key into one of the *Key 1~4* fields. Select that field number in the *Default Key* field. If the WEP key is enabled on the AP, all clients must use the same WEP key. Click ***OK***.

Note: Most wireless connection problems arise from improper WEP settings so make sure all APs and wireless stations use the same settings.

IP:

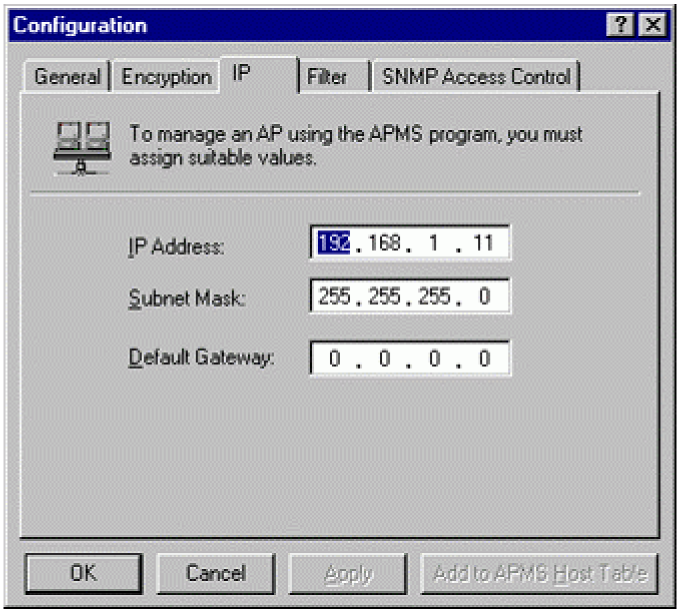
Note: These SNMP related settings are only useful for network management and remote configuration (APMS). For proper wireless connections, these settings don't have to be changed.

From the IP card (**Figure 12**) you may view or modify the Access Point's TCP/IP address, configure its subnet mask, or add a default gateway (see the note below).

Note: An AP will directly transfer SNMP respond packets (confirmation packets) to an APMS PC if it is within the same LAN (the same subnet mask). If an SNMP respond packet from an AP is destined for an APMS PC on another LAN, then the SNMP respond packet needs to go through a router-gateway. The default gateway is the path to that router. If you set the correct default gateway, then you can use an APMS manager (i.e. a PC running APMS) physically located in a different subnet to manage this AP.

IP Address	InstantWave High Rate Access Points are delivered with a default IP of 192.168.1.1 Consult your network administrator for exact settings.
Subnet Mask	InstantWave High Rate Access Points are delivered with a default subnet mask of 255.255.255.0 Consult your network administrator for exact settings.
Default Gateway	Enter the default gateway address here (if required)

If you wish to change the defaults, set each AP to its new IP address before introducing it to the open network. All APs within the same network must have the same TCP/IP subnet address.



To manage an AP using the APMS program, you must assign suitable values.

IP Address: 192 . 168 . 1 . 11

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

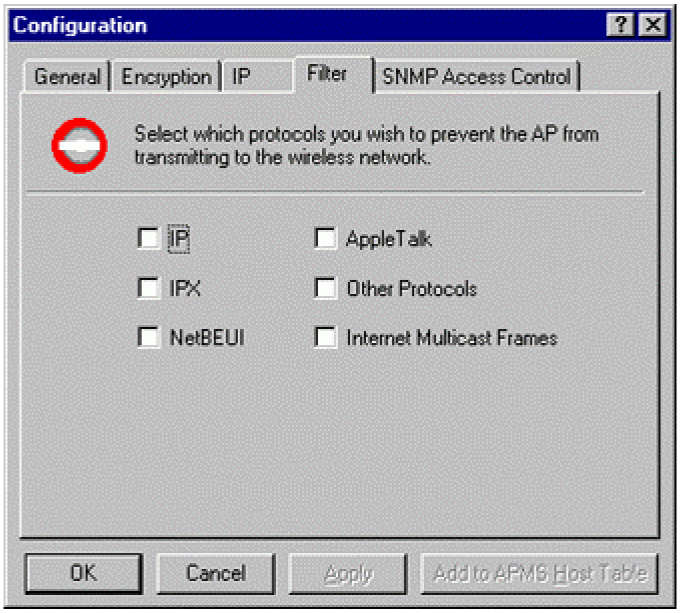
Figure 12. Configuration/IP

After making any changes, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

Note: Click **Add to APMS Host Table** *to add the configured AP to the APMS Host Table.*

Filter:

The next tab on the dialog box is *Filter* (**Figure 13**). This is a one-way protocol filtering mechanism that prevents the AP from transmitting specified protocols from a wired Ethernet LAN into the wireless LAN. If you do not require particular protocols on the wireless part of your network, you can save bandwidth by enabling the protocol filter.



Select which protocols you wish to prevent the AP from transmitting to the wireless network.

☐ IP ☐ AppleTalk
☐ IPX ☐ Other Protocols
☐ NetBEUI ☐ Internet Multicast Frames

Figure 13. Configuration/Filter

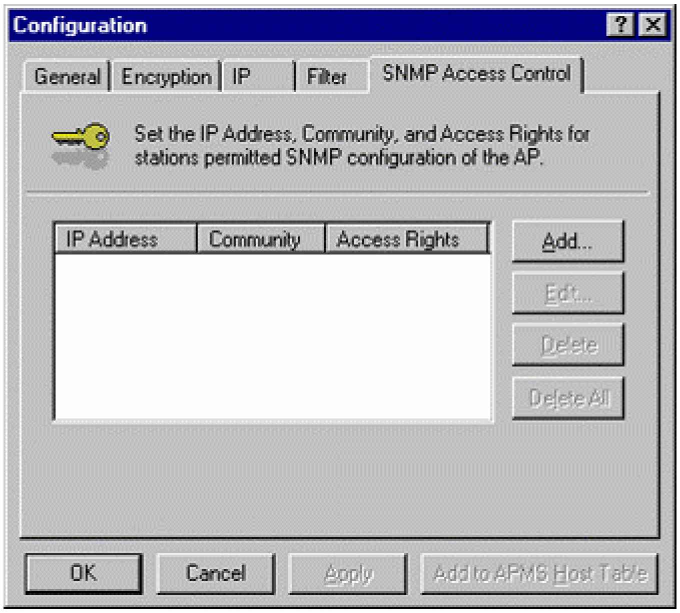
From the *Filter* card, some, all, or none of the protocols listed may be selected for filtering out:

- IP Protocol
- IPX Protocol
- NetBEUI Protocol
- AppleTalk Protocol
- Other Protocols
- Internet Multicast Frames

After selecting a protocol to be filtered, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

SNMP Access Control:

SNMP Access Control is the next tab on the box (**Figure 14**).

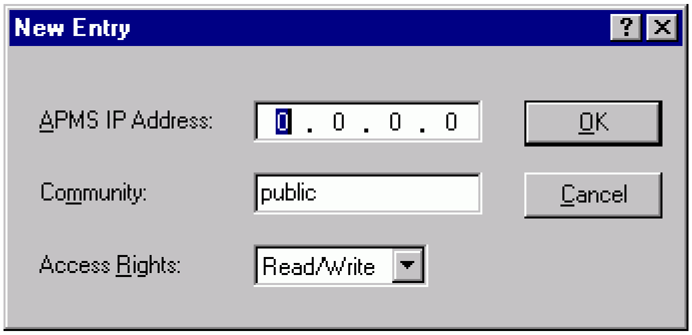


Set the IP Address, Community, and Access Rights for stations permitted SNMP configuration of the AP.

Figure 14. Configuration/SNMP Access Control

The AP’s access control is managed by a control table on the AP. The first time this box is opened, the table will be empty. This means that there are no restrictions on who can access and reconfigure the AP and any user may modify the AP’s operation. To avoid chaos on the network, access to the AP configuration should be restricted to only those for whom it is necessary.

Click ***Add*** to open the *New Entry* dialog box (**Figure 15**).


New Entry

APMS IP Address: 0 . 0 . 0 . 0

Community: public

Access Rights: Read/Write

Figure 15. New Entry

Two levels of access are available.

Read	Read-only rights. The user may read everything except the Access Control settings, but cannot alter anything
Read/Write	The user may read and alter all settings

Enter your IP address and then set your own access rights to Read/Write (see the following note).

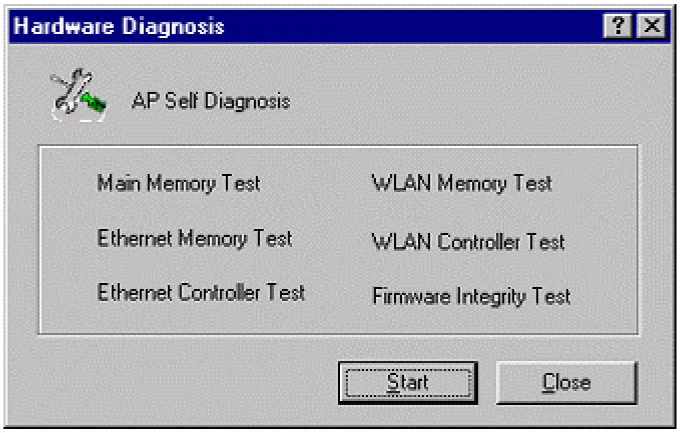
Note: Do not set all the stations in the Access Control table to Read. Once this is set and enabled, it will be difficult to modify the AP. Should this situation occur, use the AP COMFig utility to reset the configuration.

To set a stations access rights, enter a station's IP address and community string (the community string is used as a password to access the AP) and choose *Read* or *Read/Write*.

When all the settings are made, click ***OK*** to return to the *Access Control* card. On the *Access Control* card, click the ***Apply*** button to make the changes effective immediately, without closing the dialog box, or click ***OK*** to accept the changes and close the box.

Perform AP Self Diagnostic Test

On the *Service* card, click *Perform AP Self Diagnostic Test*. The *Hardware Diagnosis* screen will open (**Figure 16**).



Hardware Diagnosis

AP Self Diagnosis

Main Memory Test

WLAN Memory Test

Ethernet Memory Test

WLAN Controller Test

Ethernet Controller Test

Firmware Integrity Test

Figure 16. Hardware Diagnosis

Click ***Start*** and the tests will commence. As each item is tested, a yellow arrow will appear alongside it. If the test is successful, the arrow will change to a green tick. If a failure occurs, an “X” will appear. You can click ***Cancel*** at any time to stop the tests. When the tests have completed, the *Cancel* button changes to a *Close* button. Click ***Close*** to return to the *Service* card.

Upgrade AP Firmware

From time to time updated firmware is released and may be downloaded from our website at http://www.ndc.com.tw/support/support.htm

The updated firmware may be installed via a COM port using the AP COMFig tool. Click on ***Upgrade AP Firmware*** (Figure 9, page 12). The *Upgrade AP Firmware* dialog box will open (**Figure 17**).

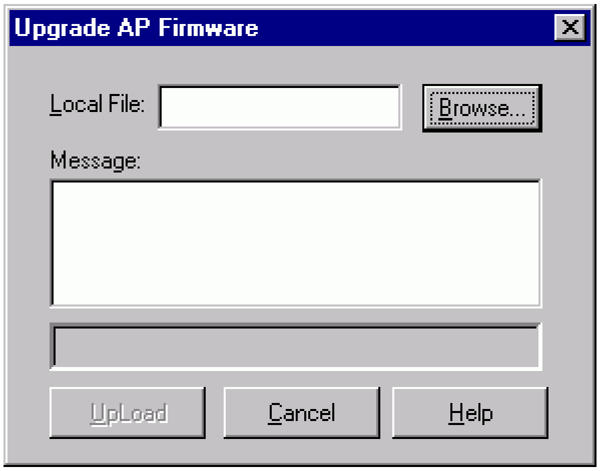
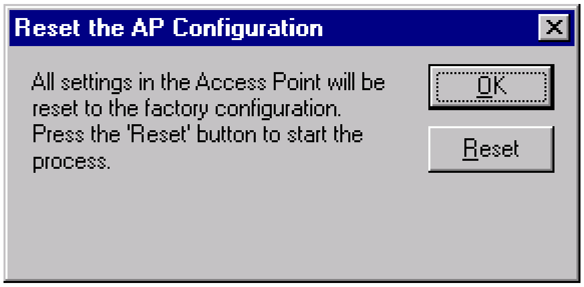

Upgrade AP Firmware

Figure 17. Upgrade AP Firmware

Use the *Browse* button to choose the file to be uploaded to the AP, or type the file location and name in the *File Name* field. The ***Upload*** button will then become enabled. Click ***Upload***. The new firmware will be loaded into the AP's flash memory area. When the file transfer is complete, click ***OK*** to begin the AP's internal firmware updating process.

Reset AP Configuration

Click ***Reset AP Configuration*** to open the screen shown in Figure 18, and click ***Reset*** to restore the factory default configuration to the Access Point.

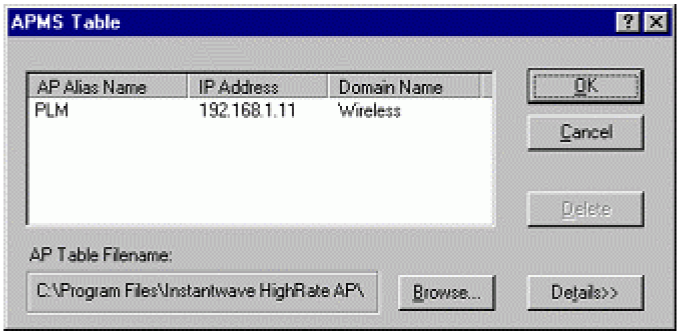

Reset the AP Configuration

All settings in the Access Point will be reset to the factory configuration. Press the 'Reset' button to start the process.

Figure 18. Reset the AP Configuration

Manage APMS Host Table

Click the *Manage APMS Host Table* button to open the *APMS Table* dialog box (**Figure 19**).



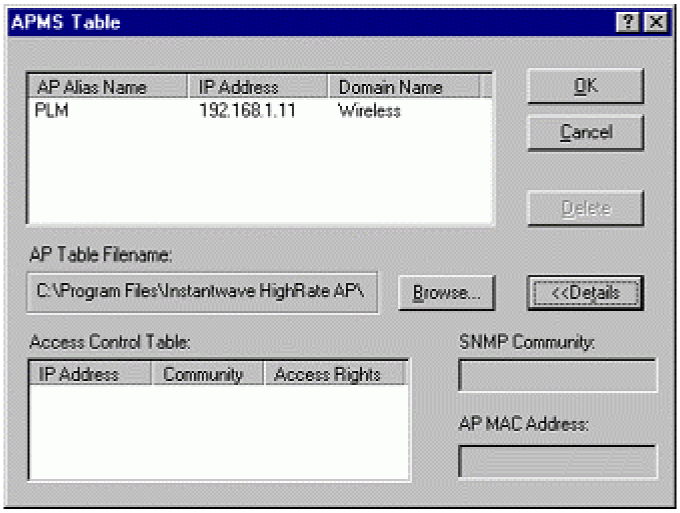
AP Alias Name	IP Address	Domain Name
PLM	192.168.1.11	Wireless

AP Table Filename: C:\Program Files\Instantwave HighRate AP\

Figure 19. APMS Table-1

From here you can view/delete all the APs added to this host table. This table can be saved and retrieved from the APMS utility so that you don't need to create such a table again in the APMS utility.

Select an AP in the table and click the ***Details*** button to view and edit it's SNMP access control settings (**Figure 20**).



AP Alias Name	IP Address	Domain Name
PLM	192.168.1.11	Wireless

AP Table Filename: C:\Program Files\Instantwave HighRate AP\

Figure 20. APMS Table-2

After making any changes, click ***OK*** to return to the *Service* card.

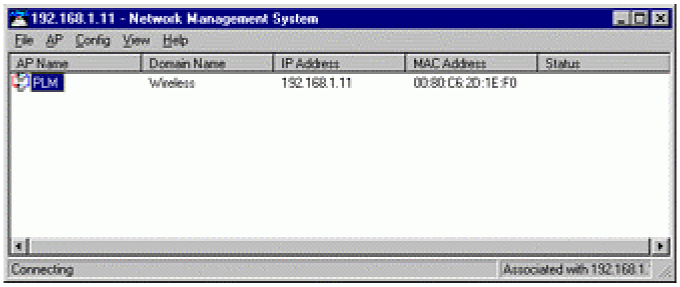
Using the Access Point Management System (Advanced Configuration and Management)

Once the AP is connected to an Ethernet network, a network administrator can connect to it from any PC on the same network via the Access Point Management System (APMS) utility.

The APMS utility is a Windows-based SNMP management tool, allowing network administrators to remotely configure and monitor APs through an Ethernet or wireless connection. The APMS management tool is intended for performing full-blown wireless network configuration and management. To launch the APMS utility, click ***Start/Programs/InstantWave High Rate AP/AP Management System.***

The program opens with the InstantWave Network Management System screen. You may now configure and monitor the APs in the wireless network from the Access Point Host Table.

The APMS Host Table is equivalent to an address book of Access Points (APs). The first time the program starts the screen will be blank.



AP Name	Domain Name	IP Address	MAC Address	Status
PLM	Wireless	192.168.1.11	00:80:C6:2D:1E:F0	

Connecting

Associated with 192.168.1.

Figure 21. Network Management System-1

At least one AP must be entered in the table to allow the local wireless adapter to connect to it. The next section explains how to add to/edit the Host Table.

Note: Right-clicking anywhere in the main window provides fast access to most of the main-menu items

To add an AP to the Host Table, use one of the methods below:

1. Load an existing Host Table by clicking ***Import Host Table*** from the File menu. You may load APs you have previously configured with the AP COMFig tool.

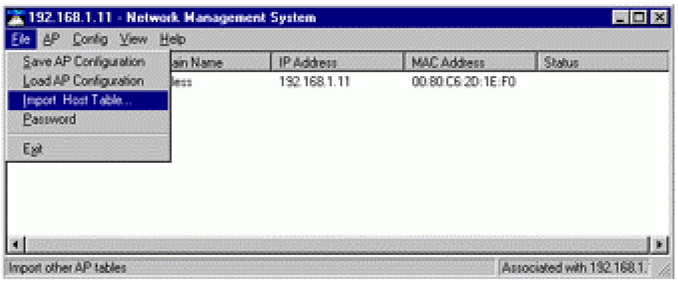


Figure 22. Network Management System-2

2. Click the *AP* main menu item to open its sub-menu and then click ***Create New AP*** (**Figure 23**).

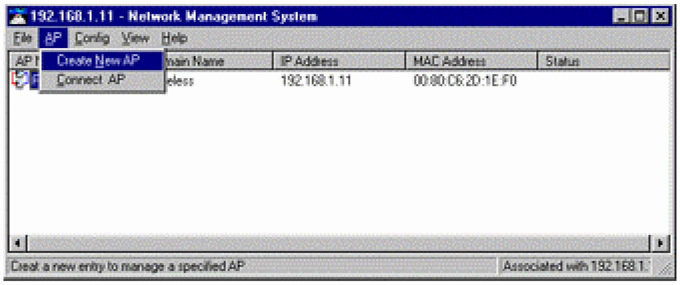


Figure 23. Network Management System-3

Input the AP's IP address and its community string (this string will be used for SNMP access control). When the information has been entered, the *OK* button will become active. Click ***OK***. Repeat the process to add more APs. To delete an AP icon from the window, first select it and then press the ***Delete*** key.

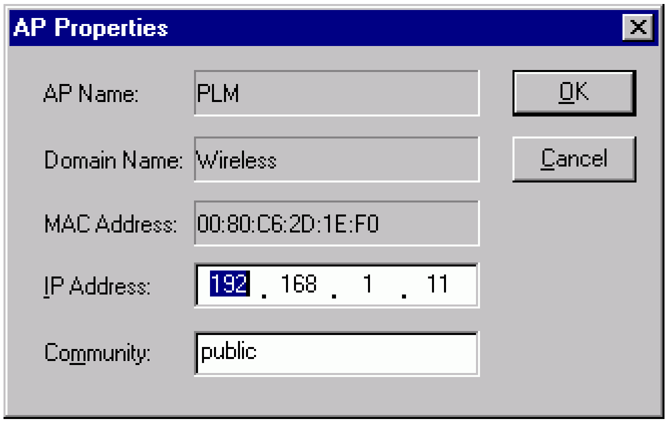
Connecting to an AP

Once a Host Table has been created, a connection can be made by double-clicking an AP's icon in the Host Table. Alternatively, click ***AP*** on the main menu and then click ***Connect AP***.

In the *Connect AP* dialog box, click on the down arrow of the AP entry field to open the dropdown AP list. Select an AP and complete the selection by clicking ***OK***. If the connection is successful the current connected AP's IP address will appear on the title bar.

AP Properties

After connecting, right-clicking on a connected AP's icon will open a menu. Click ***Properties*** to open the *AP Properties* screen (**Figure 24**).



AP Name: PLM

Domain Name: Wireless

MAC Address: 00:80:C6:2D:1E:F0

IP Address: 192 . 168 . 1 . 11

Community: public

Figure 24. AP Properties

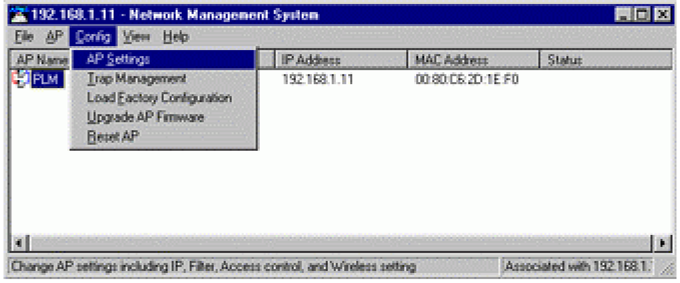
Here you may modify the IP address and Community string. Changes made here will be immediately effective.

If the connection attempt was unsuccessful, a message box will appear informing you that the request had no response. Click ***OK*** to close the message box and return to the main screen. Go through the procedure again to retry. If you cannot connect to the AP after three attempts, check that the AP information has been correctly entered in the Host Table and that the Access Point (AP) is functioning.

Managing Configurations

Config

If the AP selection is successful, the *Config* and *View* main menu items will be enabled. Click the *Config* main menu item (or right-click on the AP name in the APMS window) to open a sub-menu.



AP Name	IP Address	MAC Address	Status
PLM	192.168.1.11	00:80:C6:2D:1E:F0	

Change AP settings including IP, Filter, Access control, and Wireless setting

Associated with 192.168.1.

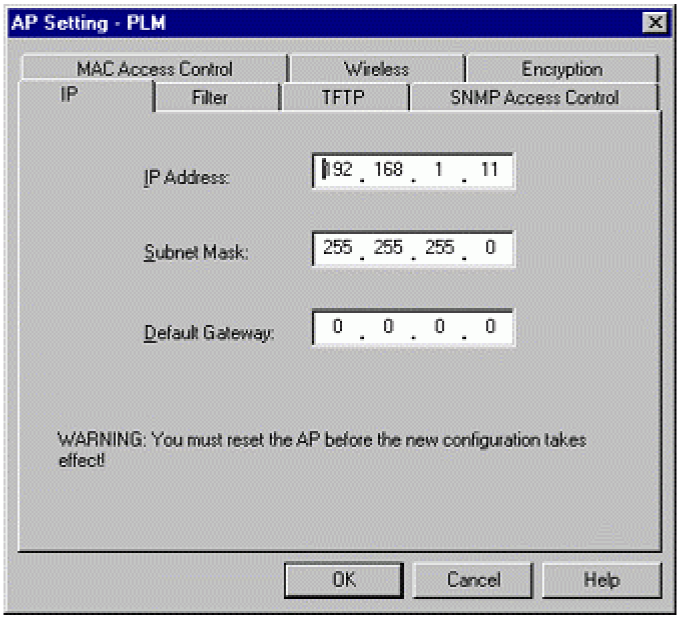
Figure 25. Config/AP Setting

The menu offers configuration options that enable you to tailor your network to suit your needs.

- AP Settings - sets the AP's IP related parameters, sets filters, sets wireless related parameters, sets AP Access Control list
- Trap Management
- Load Factory Configuration
- Upgrade AP Firmware
- Reset AP

AP Settings

Click *AP Settings* to open the *AP Settings* dialog box (**Figure 26**).



IP Address: 192 . 168 . 1 . 11

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

WARNING: You must reset the AP before the new configuration takes effect!

Figure 26. AP Settings/IP

IP:

From the IP card you may view or modify the Access Point's TCP/IP address, configure its subnet mask, or add a default gateway (see the following note).

Note: An AP will transfer SNMP respond packets (confirmation packets) to its APMS PC directly if it is within the same LAN (the same subnet mask). If an SNMP respond packet from an AP is destined for an APMS PC on another

LAN, then the SNMP respond packet needs to go through a router-gateway. The default gateway is the path to that router. If you set the correct default gateway, then you can use a PC running APMS located on a different subnet to manage this AP.

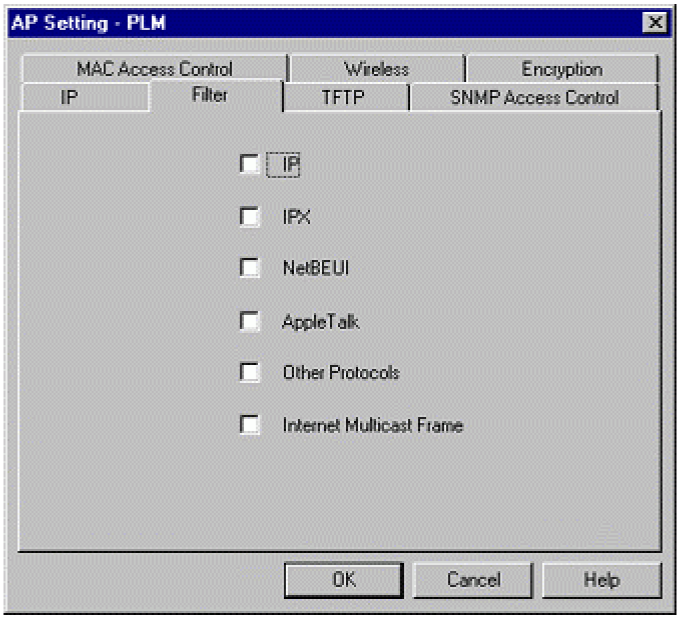
All InstantWave Access Points are delivered with a default IP of 192.168.1.1 and a default subnet mask of 255.255.255.0. If you wish to change the defaults, set each AP to its new IP address before introducing it to the open network.

Consult your network administrator for exact settings.

After making changes, click ***OK*** to return to the *Config* sub-menu and click the *Reset AP* menu item to make the changes effective.

Filter:

The second tab on the box is *Filter* (**Figure 27**). This is a one-way protocol filtering mechanism that prevents the AP from transmitting specified protocols from the wired Ethernet LAN into the wireless zone. If you do not require particular protocols on the wireless part of your network, you can save bandwidth by enabling the protocol filter.



□ IP

□ IPX

□ NetBEUI

□ AppleTalk

□ Other Protocols

□ Internet Multicast Frame

Figure 27. Filter (APMS)

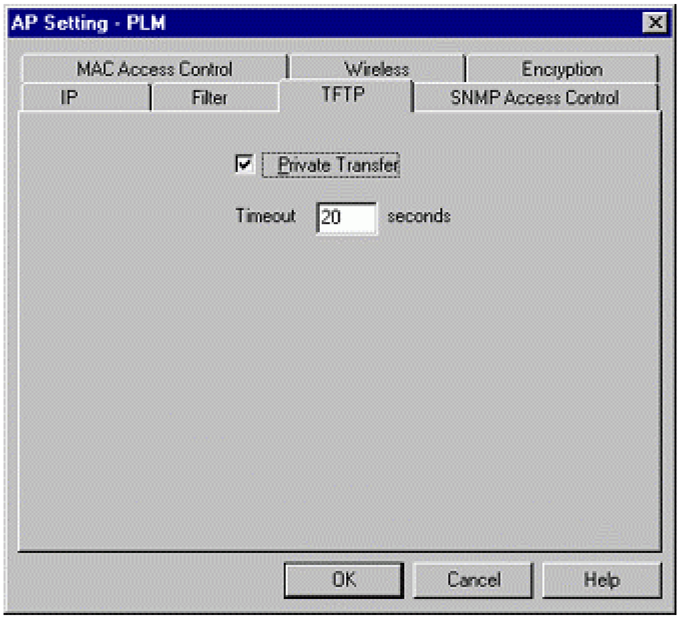
From the *Filter* card, some, all, or none of the protocols listed may be selected for filtering out:

- IP protocol
- IPX protocol
- NetBEUI protocol
- AppleTalk protocol
- Other protocols
- Internet Multicast Frames

Selecting a protocol to be filtered will activate the AP's protocol filtering immediately on clicking *OK*. Clicking *Reset AP* is not required. If, after filtering a protocol, your network is not functioning as before, it's likely the protocol is required on the network and you should disable the filter for that protocol.

TFTP:

The Access Point supports remote firmware upgrades using TFTP (Trivial File Transfer Protocol). You may customize TFTP services with the following options:



☑ Private Transfer

Timeout 20 seconds

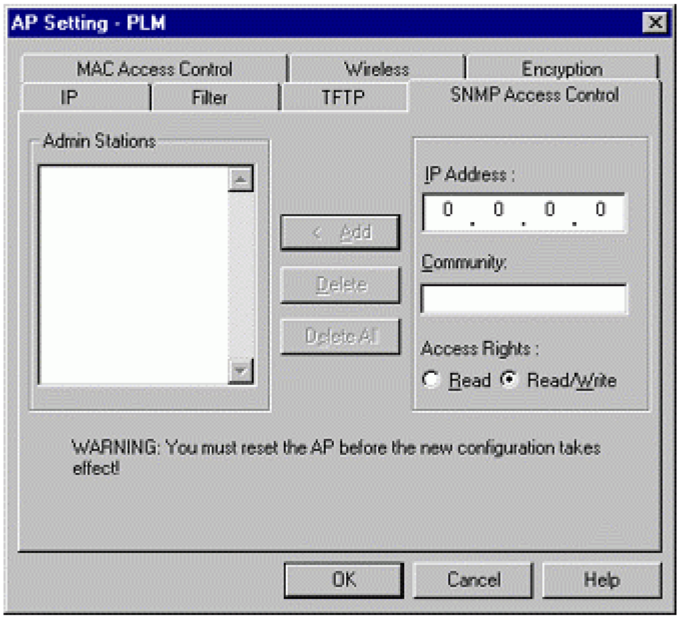
Figure 28. AP Setting/TFTP

Private Transfer:
TFTP currently has no provisions for user authentication. We suggest you keep the 'Private Transfer' option checked in order to prevent anyone other than the network administrator using the APMS program to upgrade the AP firmware. If you want to use a third party TFTP tool to upgrade the AP firmware, this option should be disabled.

Timeout:
Specifies the number of seconds TFTP waits to make sure that the sender has completed the transmission. The range is from 3 to 255 seconds.

SNMP Access Control:

SNMP Access Control is the next tab on the box (**Figure 29**). SNMP access control is managed by a control table on the AP.



IP Address : 0 . 0 . 0 . 0

Community:

Access Rights : ○ Read ● Read/Write

WARNING: You must reset the AP before the new configuration takes effect!

Figure 29. AP Setting/SNMP Access Control

The first time this box is opened, the table will be empty. This means that there are no restrictions on who can access and reconfigure the AP and any user may modify the AP's operation. Access to the AP configuration should be restricted to only those for whom it is absolutely necessary. First enter your IP address and then set your own access rights to *Read/Write* (see the note below).

Note: Do not set all the stations in the Access Control table to Read. Once this is set and enabled, it will be difficult to modify the AP. Should this situation occur, use the AP COMFig utility to re-set the configuration.

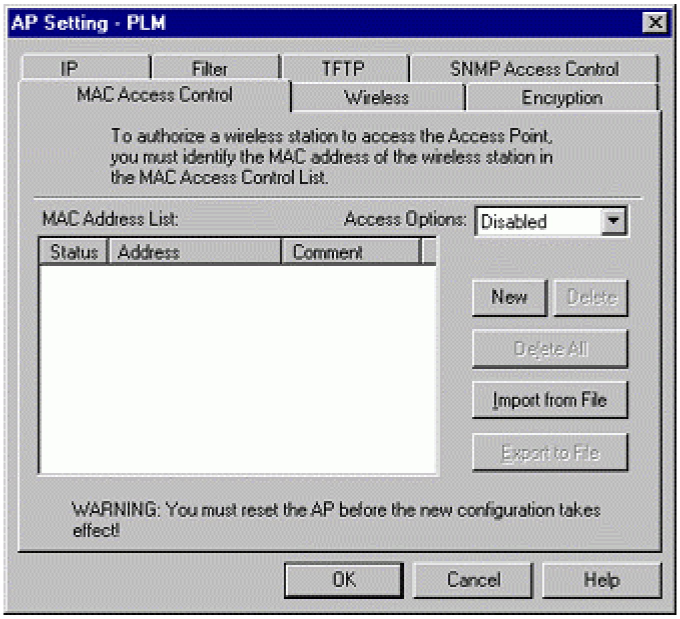
Two levels of access are available. To set access rights, enter a station's IP address and community string (the community string must be the same as the AP's in the Host Table of the APMS manager terminal, i.e. the PC running APMS) and choose *Read* or *Read/Write*.

Read	Read-only rights. The user may read everything except the Access Control settings, but cannot alter anything
Read/Write	The user may read and alter all settings

The ***Add*** button will become active. Click ***Add*** to add the information to the AP Access Control table. Click another tab to continue configuration setting or click ***OK*** to complete the AP setting. Click the *Config/Reset AP* menu item to make the changes effective.

MAC Access Control:

Limit access rights to this Access Point. You may enter up to 1000 stations (identified by their MAC addresses) into the list.



To authorize a wireless station to access the Access Point, you must identify the MAC address of the wireless station in the MAC Access Control List.

MAC Address List:

Access Options: Disabled

WARNING: You must reset the AP before the new configuration takes effect!

Figure 30. AP Setting/MAC Access Control

Access Options

MAC Address List:

Status	Disables or enables an individual entry
Address	The MAC address of a wireless station
Comment	A brief description of the wireless station

Access Options:

Disabled	Stops MAC access control, all wireless stations are allowed to associate with this access point
Accepted List	The station will be rejected if its MAC address IS NOT in the list
Denied List	The station will be rejected if its MAC address IS in the list

New:
Click ***New*** to create a new entry in the MAC Address List.

Delete:
Click ***Delete*** to remove a selected MAC address from the list.

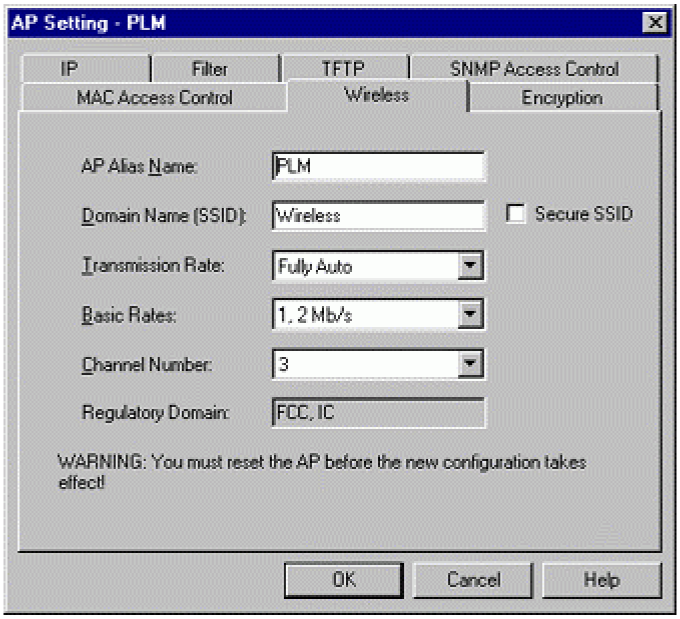
Delete All:
Click ***Delete All*** to remove all of the MAC addresses from the list.

Import from File:
Click to import a MAC access control table from a file on disk.

Export to File:
Click to export the current MAC access control table to a new file.

Wireless:

Clicking on the *Wireless* tab opens the wireless card (**Figure 31**).



AP Alias Name: PLM

Domain Name (SSID): Wireless □ Secure SSID

Transmission Rate: Fully Auto

Basic Rates: 1, 2 Mb/s

Channel Number: 3

Regulatory Domain: FCC, IC

WARNING: You must reset the AP before the new configuration takes effect!

Figure 31. AP Setting/Wireless

The *Wireless* card groups all the user configurable wireless Access Point (AP) functions. Here you may make settings as follows:

AP Alias Name	Assigns the AP a unique name
Domain Name (SSID)	This is more commonly called the Domain Name but is defined in the IEEE 802.11 Wireless Standard as SSID. Stations and APs in the same group must use the same Domain Name
Secure SSID	• Blocks a connection request without the exact SSID • Hides the SSID in outgoing beacon frames. A site survey tool will not find the AP
Transmission Rate	The transmission rate at which the data packets are transmitted by the AP. You can set this to Auto select 1 or 2Mbps, Fixed 1Mbps, Fixed 2Mbps, Fixed 5.5Mbps, Fixed 11Mbps or Full Auto (1 to 11Mbps)
Basic Rates	This value determines the basic rates used and reported for this BSS by the AP. The highest rate specified will be the rate that the AP will use when transmitting broadcast/multicast and management frames. Available options are: 1 and 2Mbps and All (1, 2, 5.5, and 11Mbps)
Channel Number	Refer to the Appendix, page 52, for a list of the channels supported in each regulatory domain
Regulatory Domain	Identifies the country where the AP is used (see the Appendix, page 52). Each Regulatory Domain has defined the channel numbers and transmission power available

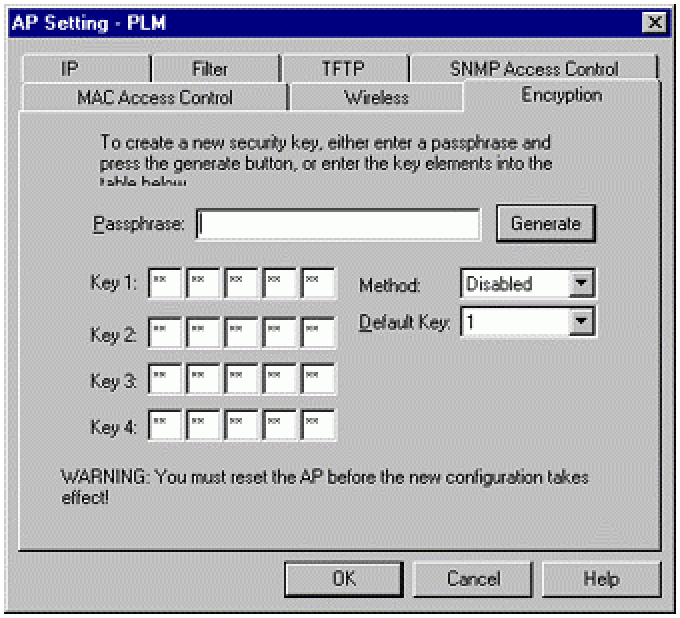
After making any changes, click ***OK*** and then click the *Reset AP* menu item.

Encryption:

Note: Most wireless connection problems arise from improper WEP settings so make sure all APs and wireless stations use the same settings.

Sets the data encryption parameters for the wireless LAN.

Click the arrow to the right of the *Method* box. The dropdown list has three options:



To create a new security key, either enter a passphrase and press the generate button, or enter the key elements into the table below

Passphrase:

Key 1: ** ** ** ** **

Key 2: ** ** ** ** **

Key 3: ** ** ** ** **

Key 4: ** ** ** ** **

Method: Disabled

Default Key: 1

WARNING: You must reset the AP before the new configuration takes effect!

Figure 32. AP Setting/Encryption

Disabled (default)
Stations communicate with this Access Point without any data encryption.

40-bit WEP
Stations communicate with this Access Point via 40-bit WEP data encryption.

128-bit WEP
Stations communicate with this Access Point via 128-bit WEP data encryption.

In order to decode the data transmissions, each wireless client on the network must use identical keys.

Key Generation - There are two ways of generating a security key.

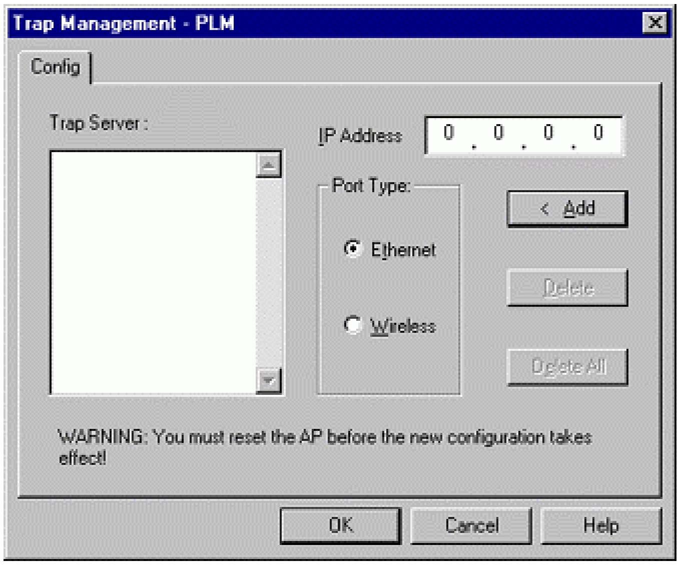
The first is by entering any text in the *Passphrase* field. Click the ***Generate*** button. For 40-bit WEP, it will generate four keys, Key 1, Key 2, Key 3, and Key 4. Select a key number from the dropdown list of the *Default Key* box. If you do not select a key, key 1 is selected, as it is the default key. For 128-bit WEP, only one key is generated. Click ***OK***.

Another WEP key generation method is to insert the key values directly from the keyboard. Enter your own key into one of the *Key 1~4* fields. Select that field number in the *Default Key* field. If the WEP key is enabled on the AP, all clients must use the same WEP key. Click ***OK***.

Trap Management

Trap Management allows you to setup the configuration of the Trap Server program. When an AP is powered on, or its Ethernet port becomes active, the AP will send messages to the assigned trap server to report these activities.

To assign a trap server, click *Trap Management* (**Figure 33**). Assign a station as a trap server by entering its IP address and network port type. Click ***Add***.
To remove a trap server from the list, highlight it and click ***Delete***. Click ***Delete All*** to remove all assigned trap servers from the list.



0 . 0 . 0 . 0

● Ethernet
○ Wireless

WARNING: You must reset the AP before the new configuration takes effect!

Figure 33. Trap Management

To view trap log information, click ***Start/Programs/InstantWave High Rate AP/Trap Server*** to open the following screen.

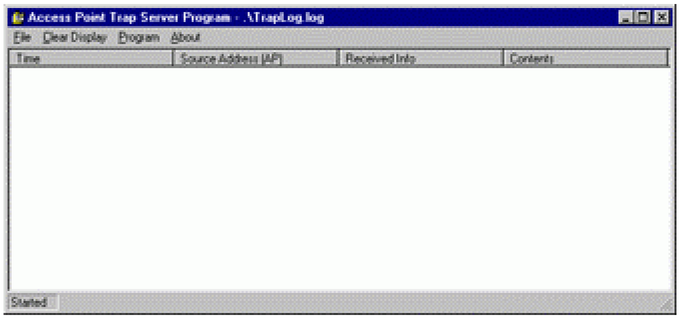


Figure 34. AP Trap Server Program

When the AP is powered on, or an Ethernet port becomes active, an event log will be generated indicating the time, the MAC ID of the reporting AP, and the activity. You may save, open, and delete log files from the *File* menu.
In the *Program* menu, select *Auto Startup After Reboot* to activate the Trap Server when the system is rebooted, or *Pause Program* to pause the Trap Server.

Load Factory Configuration

Clicking *Load Factory Configuration* opens a dialog box. Click ***OK*** to return the AP to the default settings. The default IP setting is *192.168.1.1* and the default subnet mask is *255.255.255.0*. Click the *Reset AP* menu item to make the changes effective.

Upgrade AP Firmware

The Access Point's (AP's) embedded software is burned into the flash ROM. However, an updated AP code can be installed over your LAN via the APMS program. Click on *Upgrade AP Firmware*. The *Upgrade AP Firmware* dialog box will open (**Figure 35**).

Use the *Browse* button to choose the file to be uploaded to the AP, or type the file name and path in the *Local File* field.

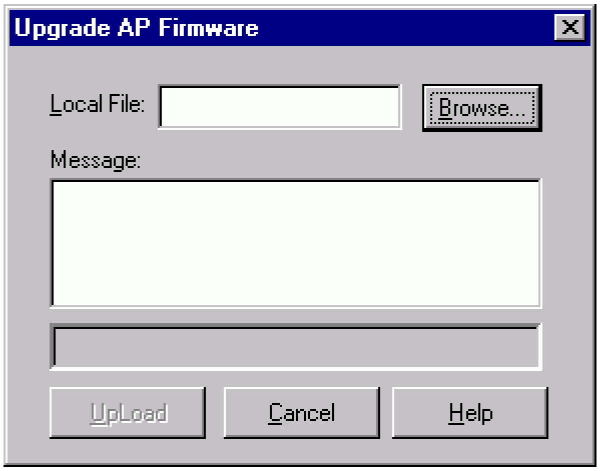


Figure 35. Upgrade AP Firmware

The ***Upload*** button will then become enabled. Click ***Upload*** to start uploading the file to the Access Point. The APMS and the AP's built-in Trivial File Transfer Protocol (TFTP) command will upload the new executable into the AP's flash memory area. If the upload activity fails, an error message will be shown on the message box.

Resetting the AP will take about 30 seconds. During this time, the APMS program will not be able to query the AP via the SNMP protocol and the AP will not be available to other stations. If you try to access it, the APMS program will display a "No response from the AP" message.

When the file transfer is complete, click ***OK*** to close the window.

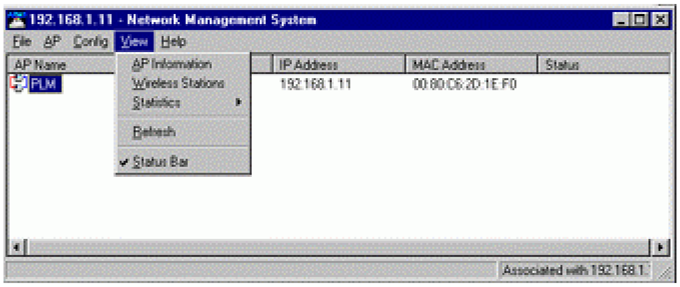
Reset AP

After changing the AP's IP, Access Control, or Wireless options, the AP needs to be reset to enable the new settings. Prior to exiting the APMS program, or selecting a different AP, click the *Reset AP* menu item. A confirmation window will open. Click ***OK*** to reset the AP or ***Cancel*** to abort the reset command.

Viewing InstantWave High Rate Information and Statistics

View

The menu items under *View* provide read-only information and statistics. To customize the screen view, right-click in the main screen to open a context sensitive menu. Select your preferred view, i.e. Icons, List, Details, etc.



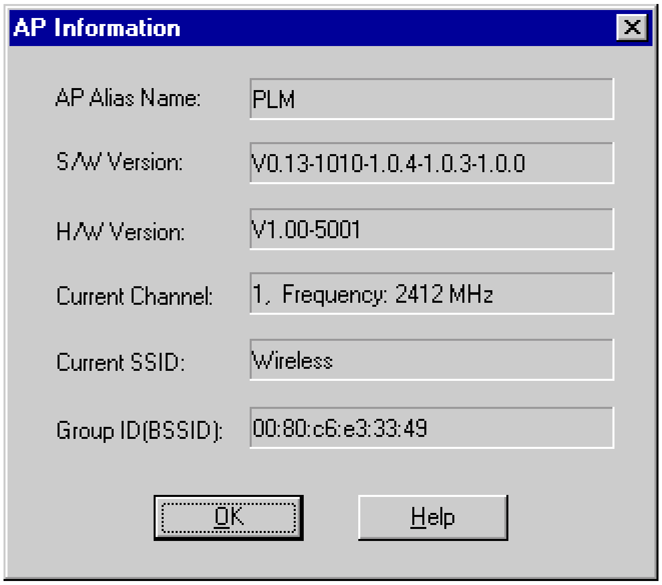
AP Name	IP Address	MAC Address	Status
PLM	192.168.1.11	00:80:C6:2D:1E:F0	

Figure 36. View Menu

The Status bar at the bottom of the screen shows the connecting status. When the bar shows *Ready*, *Associated* will appear on the bar along with the IP address of the associated AP.

AP Information

Clicking *AP Information* opens a window displaying the AP's system information (**Figure 37**). The information shown is read-only.



AP Alias Name: PLM

S/W Version: V0.13-1010-1.0.4-1.0.3-1.0.0

H/W Version: V1.00-5001

Current Channel: 1, Frequency: 2412 MHz

Current SSID: Wireless

Group ID(BSSID): 00:80:c6:e3:33:49

Figure 37. AP Information

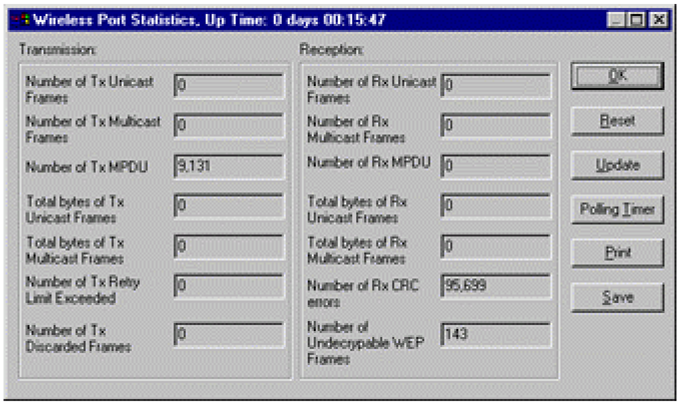
When finished viewing AP information, click ***OK*** to close the window.

Wireless Stations

The *Connected Wireless Stations* window lists all the currently associated wireless station's Media Access Control (MAC) addresses. When finished viewing, click ***OK*** to close the window.

Statistics

Clicking statistics opens a sub-menu with two options: Wireless Port and Ethernet Port. A list of Tx and Rx statistics data follows.



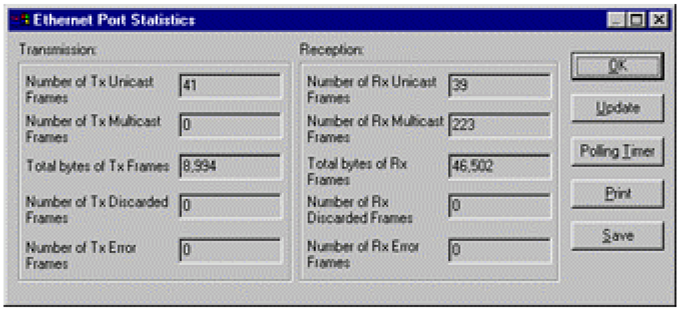
Transmission:

Number of Tx Unicast Frames: 0
Number of Tx Multicast Frames: 0
Number of Tx MPDU: 9,131
Total bytes of Tx Unicast Frames: 0
Total bytes of Tx Multicast Frames: 0
Number of Tx Retry Limit Exceeded: 0
Number of Tx Discarded Frames: 0

Reception:

Number of Rx Unicast Frames: 0
Number of Rx Multicast Frames: 0
Number of Rx MPDU: 0
Total bytes of Rx Unicast Frames: 0
Total bytes of Rx Multicast Frames: 0
Number of Rx CRC errors: 95,699
Number of Undecrypable WEP Frames: 143

Figure 38. Wireless Port Statistics



Transmission:

Number of Tx Unicast Frames: 41
Number of Tx Multicast Frames: 0
Total bytes of Tx Frames: 8,994
Number of Tx Discarded Frames: 0
Number of Tx Error Frames: 0

Reception:

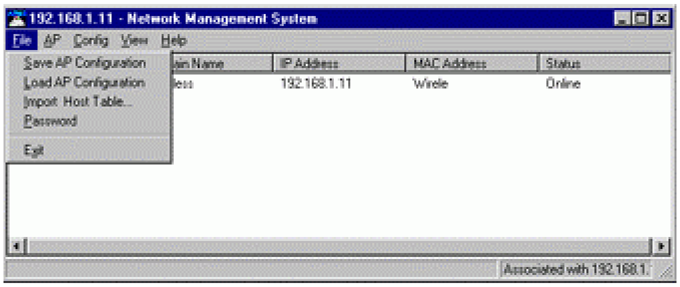
Number of Rx Unicast Frames: 39
Number of Rx Multicast Frames: 223
Total bytes of Rx Frames: 46,502
Number of Rx Discarded Frames: 0
Number of Rx Error Frames: 0

Figure 39. Ethernet Port Statistics

These statistics will be lost when the Access Point (AP) reboots or is reset. To poll for new statistics click on the *Polling Timer* button. Set the time period (in seconds) and click ***OK*** to close the box. Click ***Update*** to start the polling sequence. The statistics shown may be saved to a file or printed. Click ***OK*** to return to the main menu.

Saving the AP's Configuration to a File

After the targeted AP has connected successfully, the AP's configuration can be saved as a WLN file in text format. To do this, first click on the *File* main menu item. From the sub-menu click ***Save AP Configuration***. A standard Windows *Save As* dialog box will appear. Enter a file name, choose a location for the file, and click ***OK***.

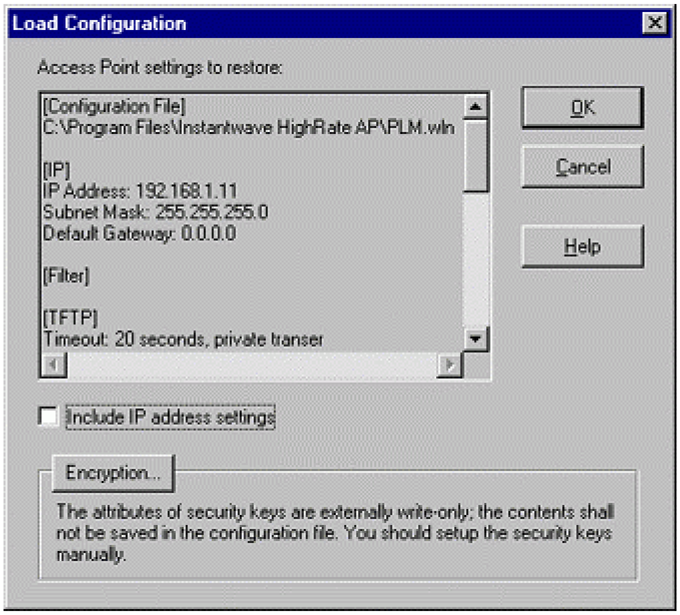


ain Name	IP Address	MAC Address	Status
less	192.168.1.11	Wirele	Online

Figure 40. Save AP Configuration

Loading the AP's Configuration from a File

To load a configuration file (.WLN) to the Access Point, on the *File* menu, click ***Load AP Configuration***. Select a configuration file and open it. The following dialog box will open and display the detailed settings.



Access Point settings to restore:

```
[Configuration File]
C:\Program Files\Instantwave HighRate AP\PLM.wln

[IP]
IP Address: 192.168.1.11
Subnet Mask: 255.255.255.0
Default Gateway: 0.0.0.0

[Filter]

[TFTP]
Timeout: 20 seconds, private transer
```

□ Include IP address settings

The attributes of security keys are externally write-only; the contents shall not be saved in the configuration file. You should setup the security keys manually.

Figure 41. Load Configuration

Include IP address settings: If you want to include the IP settings, **c**heck this option (overwrites the AP's current IP settings).

Encryption

The configuration file does not contain the security key settings. The attributes of security keys are externally **write-only** and cannot be saved into the configuration file. Click ***Encryption*** to setup the security keys manually.

Password

Clicking ***Password*** opens a *Change Password* configuration box. Enter your new password and then enter it again to confirm. Click ***OK*** to close the box. Once a password is set you will be asked for it each time the APMS program is opened.

Note: The password is shared between the APMS and the AP COMFig program on the same PC.

Troubleshooting

This section provides you with some troubleshooting info should you encounter installation or operation problems on InstantWave High Rate products. If the problems still cannot be remedied after going through the Troubleshooting section, check the FAQs at http://www.ndc.com.tw/support/tech/iw_faq.htm
If you still have a problem, contact NDC technical support for assistance (see Technical Support, page 47).

Before going through the following troubleshooting information, run the *AP Self Diagnostic Test* to ensure the major AP components are working.

If your problems still cannot be remedied after going through this Troubleshooting section, contact NDC technical support for assistance (see Technical Support, page 47).

Symptom	***Suggested Solutions***
The Power LED on the AP is OFF.	1. Make sure the power adapter is firmly connected to the power outlet and the AP power connector.
The InstantWave HR APMS utility cannot detect an InstantWave HR AP on the same network.	1. Make sure the AP is powered on and connected to an Ethernet work. Check the IP addresses assigned to the AP and APMS terminal PC. They should be in the same subnet and unique. For example, if the AP's IP address is 192.168.1.5 with a mask of 255.255.255.0, then the PC's IP address should be 192.168.1.x with a mask of 255.255.255.0. Consult your network administrator for exact settings.
The AP powers up, but the Ethernet Link LED is OFF (no connection to an Ethernet network).	Make sure: 1. The Ethernet cable is connected firmly to both the AP and Hub/Switch. 3. The Hub/Switch is powered on. 4. Your Hub/Switch port may be set to the "Uplink" position. Set it to the normal position.
The Status LED on the AP panel is Red and flashing.	Restart (power cycle) the AP and check the Status LED again. If it is still flashing, you need to return the AP to the reseller for repair.

A wireless PC cannot associate with the AP, even though the link quality is perfect and the taskbar indicator is green.	Make sure your wireless PC is using a WiFi compliant adapter and has the same SSID and security settings as the AP. 1. SSID: The 'Domain Name (SSID)' is case-sensitive and must be the same as that of the AP. See Figure 10, page 13 (AP COMFig) or Figure 31, page 34 (APMS). 2. Security: You need to have the same security setting (Disabled, 40-bit WEP, or 128-bit WEP) and WEP key (if 40-bit or 128-bit WEP is selected). See *Encryption*, page 15 (AP COMFig) or page 36 (APMS).
Transmission performance is slow or erratic.	1. Move your wireless PC closer to the AP to find a better signal. If the signal is still weak, change the direction of the antenna slightly. 2. There may be interference, possibly caused by a microwave oven, 2.4GHz wireless phone, or metal objects. Move these interference sources or change the location of the wireless PC or AP. 3. Change the wireless channel on the AP. See Figure 10, page 13 (AP COMFig) or Figure 31, page 34 (APMS). 4. Check the AP antenna, connectors, and cabling are firmly connected.
The AP and wireless adapter are working, but the PC cannot connect to the Ethernet network via the AP.	1. The MAC access control function is enabled and this PC is denied access. See Figure 30, page 32. 2. The Protocol Filter has blocked required protocols, e.g. TCP/IP to the PC. Uncheck these protocols from the filtering list. See Figure 13, page 19 (AP COMFig) or Figure 27, page 29 (APMS). 3. The IP settings on the PC are not correct.
The AP cannot be detected by the Site Survey tool	1. The distance between the AP and wireless PC is too great. 2. The Secure SSID setting has been set. See Figure 10, page 13 (AP COMFig) or Figure 31, page 34 (APMS).

Technical Support

Support from Your Network Supplier

If assistance is required, call your supplier for help. Have the following information ready before you make the call.

1. LED status
2. A list of the product hardware (including revision levels), and a brief description of the network structure
3. Details of recent configuration changes, if applicable

Support from NDC

If you have any problems that you cannot resolve with the information in troubleshooting, or the FAQs at
http://www.ndc.com.tw/support/tech/iw_faq.htm
please note the following information and contact our technical support team:

- What you were doing when the error occurred
- What error messages you saw
- Whether the problem can be reproduced
- The serial number of the product
- The firmware version and the debug information

NDC Technical Support is available via:
E-mail: techsupt@ndc.com.tw

For other information about NDC, please visit us at: www.ndc.com.tw

NDC Limited Warranty

Hardware

NDC warrants its products to be free of defects in workmanship and materials, under normal use and service, for a period of 12 months from the date of purchase from NDC or its Authorized Reseller, and for the period of time specified in the documentation supplied with each product.

Should a product fail to be in good working order during the applicable warranty period, NDC will, at its option and expense, repair or replace it, or deliver to the purchaser an equivalent product or part at no additional charge except as set forth below. Repair parts and replacement products are furnished on an exchange basis and will be either reconditioned or new. All replaced products and parts will become the property of NDC. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

NDC shall not be liable under this warranty if its testing and examination disclose that the alleged defect in the product does not exist or was caused by the purchaser's, or any third party's misuse, neglect, improper installation or testing, unauthorized attempt to repair or modify, or any other cause beyond the range of the intended use, or by accident, fire, lightning, or other hazard.

Software

Software and documentation materials are supplied "as is" without warranty as to their performance, merchantability, or fitness for any particular purpose. However, the media containing the software is covered by a 90-day warranty that protects the purchaser against failure within that period.

Limited Warranty Service Procedures

Any product (1) received in error, (2) in a defective or non-functioning condition, or (3) exhibiting a defect under normal working conditions, can be returned to NDC by following these steps:

You must prepare:

- Dated proof of purchase
- Product model number & quantity
- Product serial number
- Precise reason for return
- Your name/address/email address/telephone/fax

1. Inform the distributor or retailer.
2. Ship the product back to the distributor/retailer with prepaid freight. The purchaser must pay the shipping fee from the distributor/retailer to NDC. Any package sent C.O.D. (Cash On Delivery) will be refused.

3. Charges: Usually RMA (Returned Material Authorization) items will be returned to the purchaser via airmail, prepaid by NDC. If returned by another carrier, the purchaser will pay the difference. A return freight and handling fee will be charged to the purchaser if NDC determines that there was "No Problem Found" or that the damage was caused by the user.

Warning

NDC is not responsible for the integrity of any data on storage equipment (hard drives, tape drives, floppy diskettes, etc.). We strongly recommend that our customers back their data up before sending such equipment in for diagnosis or repair.

Services after Warranty Period

After the warranty period expires, all products can be repaired for a reasonable service charge. The shipping charges to and from the NDC facility will be borne by the purchaser.

Return for Credit

In the case of a DOA (Dead on Arrival) or a shipping error, a return for credit will automatically be applied to the purchaser's account, unless otherwise requested.

Limitation of Liability

All expressed and implied warranties of a product's merchantability, or of its fitness for a particular purpose, are limited in duration to the applicable period as set forth in this limited warranty, and no warranty will be considered valid after its expiration date.

If this product does not function as warranted, your sole remedy shall be repair or replacement as provided for above. In no case shall NDC be liable for any incidental, consequential, special, or indirect damages resulting from loss of data, loss of profits, or loss of use, even if NDC or an authorized NDC distributor/dealer has been advised of the possibility of such damages, or for any claim by any other party.

Specifications

General

Regulatory Compliance	FCC Part 15 Class B. (US)
Standards	Wireless LAN: IEEE 802.11b, Wi-Fi Compliant Ethernet: IEEE 802.3
Data Rate	11Mbps/5.5Mbps/2 Mbps/1Mbps auto fallback
Communication Method	Half-Duplex
Security	40-bit/128-bit WEP Data Encryption
LED Indicators	Power, Ethernet Activity, Ethernet Link, Wireless Activity, Wireless Link
Interfaces/Connectors	10Base-T: RJ-45 RS-232C: V.24 compliance. D-SUB 9 pin
Power	Power Voltage: DC 5.1Volt ± 5 % AC Adapter: AC 100V~240V Power Consumption: 5.1Volt, 1.0 A (Typical)
Dimensions	138 x 114 x 37mm (5.43 x 4.49 x 1.46in)

Wireless Specifications

Emission Type	Direct Sequence Spread Spectrum
RF Frequency Range	2471MHz ~ 2497MHz – Japan Band 2400MHz ~ 2483.5MHz – North America, Europe, and Extended Japan Band 2445MHz ~ 2475MHz – Spain 2446.5MHz ~ 2483.5MHz – France
Transmitter	RF Output Power: 20 dBm Frequency Stability: Within ± 25ppm Data Modulation Type: BPSK (1Mbps)/QPSK (2/5.5/11Mbps) Data Modulation Speed: 11Mbps/5.5Mbps/2Mbps/1Mbps with Auto Fallback
Antenna Type	Dual Dipole Diversity Antenna

Software

SNMP Functions	Configuration via COM port and Configuration and management via SNMP in a Windows environment through Ethernet. MIB II (RFC 1213), Bridge MIB (RFC 1493) Enterprise MIB Trap Filter
Security	Data encryption Access control Password assignment and rights
Firmware Upgrade	Access Point firmware upgrade via COM port, Ethernet, wireless, or PPP connection from remote site

Environment

Temperature	Operating: 0°C ~ +50°C (Except RF output power and sensitivity) Storage: -30°C ~ +70°C
Humidity	85% at 40°C

Appendix

This appendix lists the channels supported by the world's regulatory domains.

The channel numbers, channel center frequencies, and regulatory domains are shown in the table.

Channel Number	*Center Frequency (MHz)*	*FCC/ Canada*	*ETSI*	*Spain*	*France*	*Japan*
1	2412	O	O			O
2	2417	O	O			O
3	2422	O	O			O
4	2427	O	O			O
5	2432	O	O			O
6	2437	O	O			O
7	2442	O	O			O
8	2447	O	O			O
9	2452	O	O			O
10	2457	O	O	O	O	O
11	2462	O	O	O	O	O
12	2467		O		O	O
13	2472		O		O	O
14	2484					O

EC DECLARATION OF CONFORMITY

For the following equipment:

Product Name : InstantWave Wireless Access Point

Model Number : NWH650

is hereby confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to R&TTE Directive(99/ 5/ EC). For the evaluation regarding the electromagnetic compatibility, the following standards were applied.

The product meets or exceeds the following EMC standards:

EN 300 328 (November 1996/A1 (July 1997))

EN 300 826 (November 1997)

En 60950:1992 + A1:1993 + A2:1993 + A3:1995 + A4:1996 + A11:1997

The manufacturer/importer is responsible for this declaration:

Company Name : NDC Europe

Company Address : 1, Earlsfort Centre
Hatch Street
Dublin 2, Ireland

Person authorized to make this declaration:

Name : Changhua Chiang

Position/Title : President & CEO

November 15, 2001

Date

Legal Signature

Index